We claim:

1. A smart card, comprising:

communication unit to communicate with the outside;

information accumulating unit to accumulate data and a program; and

arithmetic processing unit to perform information processing,

wherein:

said information accumulating unit stores value data, a transfer key used to update the value data, a transfer key identifier used to judge whether the transfer key is newer or older in accordance with a value of the transfer key identifier, an update key used to update the transfer key, and an upper limit of transfer key identifier that represents an upper limit of the transfer key identifier that can be stored by the smart card;

said arithmetic processing unit updates the transfer key identifier and the transfer key by performing encryption using the update key on the basis of common-key cryptography; and

said arithmetic processing unit then updates the value data by performing encryption using the transfer key on the basis of the common-key cryptography.

2. A smart card according to claim 1, wherein

said arithmetic processing unit comprises the steps

of:

if command data that requests transmission of card information is received, transmitting the transfer key identifier to the outside as response data;

if command data that requests update permission of the transfer key is received, generating a first random number and transmitting the first random number to the outside as response data;

if the command data which requests to obtain the transfer key, and which stores a second random number, is received, transmitting first encrypted data, into which the second random number, the transfer key identifier, and the transfer key are encrypted by use of the update key on the basis of common-key cryptography, to the outside as response data; and

if command data which requests update of the transfer key, and which stores second encrypted data, is received, decrypting the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and if the first data is equivalent to the first random number, and if a value of the second data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the second data, and updating a value of the transfer key to a value of the third data.

3. A smart card, comprising:

communication unit to communicate with the outside;

information accumulating unit to accumulate data and a program; and

arithmetic processing unit to perform information processing,

wherein:

said information accumulating unit stores value data, a transfer key used to update the value data, a transfer key identifier used to judge whether the transfer key is newer or older in accordance with a value of the transfer key identifier, a first public key certificate including a first public key, which is used to update the transfer key, a secret key corresponding to the first public key, and an upper limit of transfer key identifier that represents an upper limit of the transfer key identifier which can be stored by the smart card;

said arithmetic processing unit updates the transfer key identifier and the transfer key by performing encryption using the first public key certificate and the secret key on the basis of public-key cryptography; and

said arithmetic processing unit then updates the value data by performing encryption using the transfer key on the basis of common-key cryptography.

4. A smart card according to claim 3, wherein:

said arithmetic processing unit comprises the steps

of:

if command data that requests transmission of card information is received, transmitting the transfer key identifier and the first public key certificate to the outside as response data;

if command data which requests update permission of the transfer key, and which stores a second public key certificate including a second public key, is received, generating a first random number and transmitting the first random number to the outside as response data;

if command data which requests to obtain the transfer key, and which stores a second random number and a third public key certificate including a third public key, is received, first creating first encrypted data into which the transfer key identifier and the transfer key are encrypted by use of the third public key on the basis of public-key cryptography, next creating first digital signature data from the first encrypted data and the second random number by use of the secret key on the basis of public-key cryptography, and lastly transmitting the first encrypted data and the first digital signature data to the outside as response data; and

if command data which requests update of the transfer key, and which stores second encrypted data and second digital signature data, is received, first checking the second digital signature data by use of the second

public key on the basis of public-key cryptography, next decrypting the second encrypted data by use of the secret key on the basis of public-key cryptography to extract first data and second data, and lastly if a value of the first data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the first data, and updating a value of the transfer key to a value of the second data.

5. A smart card, comprising:

communication unit to communicate with the outside;

information accumulating unit to accumulate data and a program; and

arithmetic processing unit to perform information processing,

wherein:

said information accumulating unit stores value data, a transfer key used to update the value data, a transfer key identifier used to judge whether the transfer key is newer or older in accordance with a value of the transfer key identifier, an update key used to update the transfer key, an update key identifier used to judge whether the update key is newer or older in accordance with a value of the update key identifier, a first public key certificate including a first public key, which is used to update the transfer key, a secret key corresponding to the first

public key, and an upper limit of transfer key identifier that represents an upper limit of the transfer key identifier which can be stored by the smart card;

said arithmetic processing unit updates the transfer key by use of the update key on the basis of common-key cryptography, or updates the transfer key by use of the first public key certificate and the secret key on the basis of common-key cryptography; and

said arithmetic processing unit then updates the value data by performing encryption using the transfer key on the basis of the common-key cryptography.

6. A smart card according to claim 5, wherein:

said arithmetic processing unit comprises the steps of:

if command data that requests transmission of card information is received, transmitting the transfer key identifier, the update key identifier, and the first public key certificate to the outside as response data;

if command data that requests update permission of the transfer key is received, generating a first random number and transmitting the first random number to the outside as response data;

if the command data which requests to obtain the transfer key, and which stores a second random number, is received, transmitting first encrypted data, into which the second random number, the transfer key identifier, and the

transfer key are encrypted by use of the update key on the basis of common-key cryptography, to outside as response data; and

if command data which requests update of the transfer key, and which stores second encrypted data, is received, first decrypting the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and next if the first data is equivalent to the first random number, and if a value of the second data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the second data, and updating a value of the transfer key to a value of the third data.

7. A smart card according to claim 5, wherein:

said arithmetic processing unit comprises the steps of:

if command data that requests transmission of card information is received, transmitting the transfer key identifier, the update key identifier, and the first public key certificate to the outside as response data;

if command data which requests update permission of the transfer key, and which stores a second public key certificate including a second public key, is received, generating a first random number and transmitting the first random number to the outside as response data;

if command data which requests to obtain the transfer key, and which stores a second random number and a third public key certificate including a third public key, is received, first creating first encrypted data into which the transfer key identifier and the transfer key are encrypted by use of the third public key on the basis of public-key cryptography, next creating first digital signature data from the first encrypted data and the second random number by use of the secret key on the basis of public-key cryptography, and lastly transmitting the first encrypted data and the first digital signature data to outside as response data; and

if command data which requests update of the transfer key, and which stores second encrypted data and second digital signature data, is received, first checking the second digital signature data by use of the second public key on the basis of public-key cryptography, next decrypting the second encrypted data by use of the secret key on the basis of public-key cryptography to extract first data and second data, and lastly if a value of the first data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the first data, and updating a value of the transfer key to a value of the second data.

8. A smart card, comprising:

communication unit to communicate with the outside;

information accumulating unit to accumulate data and a program; and

arithmetic processing unit to perform information processing,

wherein:

said information accumulating unit stores value data, one or more transfer keys used to update the value data, a selection transfer key identifier used to identify the transfer key currently selected, and an update key used to update the transfer key;

said arithmetic processing unit updates the selection transfer key identifier by performing encryption using the update key on the basis of common-key cryptography; and

said arithmetic processing unit then updates the value data by performing encryption using the transfer key on the basis of common-key cryptography.

9. A smart card according to claim 8, wherein:

said arithmetic processing unit comprises the steps of:

if command data that requests transmission of card information is received, transmitting the selection transfer key identifier to the outside as response data;

if command data that requests update permission of the transfer key is received, generating a first random

number and transmitting the first random number to the outside as response data;

if the command data which requests to obtain the transfer key, and which stores a second random number, is received, transmitting first encrypted data, into which the second random number, the selection transfer key identifier, and the transfer key are encrypted by use of the update key on the basis of common-key cryptography, to the outside as response data; and

if command data which requests update of the transfer key, and which stores second encrypted data, is received, decrypting the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and if the first data is equivalent to the first random number, and if a value of the second data is equivalent to one of values of the transfer key identifiers, updating a value of the selection transfer key identifier to a value of the second data.

10. A settlement terminal comprising:

first card reading and writing unit having a function of communicating with a first smart card that holds first value data inside;

second card reading and writing unit having a function of communicating with a second smart card that holds second value data inside; and

arithmetic processing unit to update the first value data and the second value data by performing encryption between the first smart card and the second smart card using the first transfer key held by the first smart card and the second transfer key held by the second smart card on the basis of common-key cryptography,

wherein:

said arithmetic processing unit comprises the steps of:

obtaining, from the first smart card, a first transfer key identifier used to judge whether the first transfer key is newer or older in accordance with a value of the first transfer key identifier, and obtaining, from the second smart card, a second transfer key identifier used to judge whether the second transfer key is newer or older in accordance with a value of the second transfer key identifier; and

comparing the value of the first transfer key identifier with the value of the second transfer key identifier, and if the values differ from each other, updating either a value of the transfer key held by the first smart card or a value of the transfer key held by the second smart card on the basis of common-key cryptography, and then updating the value data on the basis of common-key cryptography.

11. A settlement terminal according to claim 10,

wherein:

said arithmetic processing unit comprises the steps of:

obtaining a random number from the first smart card;

after transmitting the random number to the second smart card, obtaining, from the second smart card, encrypted data into which the random number, the second transfer key identifier, and the second transfer key are encrypted on the basis of common-key cryptography; and

transmitting the encrypted data to the first smart card to update the value of the first transfer key identifier to the value of the second transfer key identifier, and to update the value of the first transfer key to the value of the second transfer key.

12. A settlement terminal comprising:

first card reading and writing unit having a function of communicating with a first smart card that holds first value data inside;

second card reading and writing unit having a function of communicating with a second smart card that holds second value data inside; and

arithmetic processing unit to update the first value data and the second value data by performing encryption between the first smart card and the second smart card using the first transfer key held by the first smart card and the second transfer key held by the second smart card

on the basis of common-key cryptography,

wherein:

said arithmetic processing unit comprises the steps of:

obtaining, from the first smart card, a first public key certificate, and a first transfer key identifier used to judge whether the first transfer key is newer or older in accordance with a value of the first transfer key identifier, and obtaining, from the second smart card, a second public key certificate, and a second transfer key identifier used to judge whether the second transfer key is newer or older in accordance with a value of the second transfer key identifier; and

comparing the value of the first transfer key identifier with the value of the second transfer key identifier, and if the values differ from each other, updating either the value of the transfer key held by the first smart card or the value of the transfer key held by the second smart card on the basis of public-key cryptography, and then updating the value data on the basis of common-key cryptography.

13. A settlement terminal according to Claim 12, wherein:

said arithmetic processing unit comprises the steps of:

after transmitting the second public key

certificate to the first smart card, obtaining a random number from the first smart card;

after transmitting the first public key certificate and the random number to the second smart card, obtaining, from the second smart card, encrypted data into which the second transfer key identifier and the second transfer key are encrypted on the basis of public-key cryptography, and digital signature data created from the random number and the encrypted data on the basis of public-key cryptography; and

then transmitting the digital signature and the encrypted data to the first smart card to updates the value of the first transfer key identifier to the value of the second transfer key identifier, and to update the value of the first transfer key to the value of the second transfer key.

14. A settlement terminal comprising:

first card reading and writing unit having a function of communicating with a first smart card that holds first value data inside;

second card reading and writing unit having a function of communicating with a second smart card that holds second value data inside; and

arithmetic processing unit to update the first value data and the second value data by performing encryption between the first smart card and the second smart card

using the first transfer key held by the first smart card and the second transfer key held by the second smart card on the basis of common-key cryptography,

wherein:

said arithmetic processing unit comprises the steps of:

first obtaining, from the first smart card, a first transfer key identifier used to judge whether the first transfer key is newer or older in accordance with a value of the first transfer key identifier, a first update key identifier used to judge whether the first update key is newer or older in accordance with a value of the first update key identifier, said update key being used to update the first transfer key, and the first public key certificate, and obtaining, from the second smart card, a second transfer key identifier used to judge whether the second transfer key is newer or older in accordance with a value of the second transfer key identifier, a second update key identifier used to judge whether the second update key is newer or older in accordance with a value of the second update key identifier, said update key being used to update the second transfer key, and the second public key certificate;

if the value of the first transfer key identifier differs from the value of the second transfer key identifier, and if the value of the first update key

identifier is equivalent to the value of the second update key identifier, updating either the value of the transfer key held by the first smart card or the value of the transfer key held by the second smart card on the basis of common-key cryptography;

if the value of the first transfer key identifier differs from the value of the second transfer key identifier, and if the value of the first update key identifier differs from the value of the second update key identifier, updating either the value of the transfer key held by the first smart card or the value of the transfer key held by the second smart card on the basis of public-key cryptography; and

then updating the value data on the basis of common-key cryptography.

15. A settlement terminal according to Claim 14, wherein:

said arithmetic processing unit comprises the steps of:

if the second transfer key identifier is newer than the first transfer key identifier, and if the value of the first update key identifier is equivalent to the value of the second update key identifier, first obtaining a random number from the first smart card;

after transmitting the random number to the second smart card, obtaining, from the second smart card,

encrypted data into which the random number, the second transfer key identifier, and the second transfer key are encrypted on the basis of common-key cryptography; and

transmitting the encrypted data to the first smart card to update the value of the first transfer key identifier to the value of the second transfer key identifier, and to update the value of the first transfer key to the value of the second transfer key.

16. A settlement terminal according to claim 14, wherein:

said arithmetic processing unit comprises the steps of:

if the second transfer key identifier is newer than the first transfer key identifier, and if the value of the first update key identifier differs from the value of the second update key identifier, first transmitting the second public key certificate to the first smart card before obtaining a random number from the first smart card;

after transmitting the first public key certificate and the random number to the second smart card, obtaining, from the second smart card, encrypted data into which the second transfer key identifier and the second transfer key are encrypted on the basis of public-key cryptography, and digital signature data created from the random number and the encrypted data on the basis of public-key cryptography; and

then transmitting the digital signature and the encrypted data to the first smart card to updates the value of the first transfer key identifier to the value of the second transfer key identifier, and to update the value of the first transfer key to the value of the second transfer key.

17. A smart card that transmits/receives value data to/from another smart card, said smart card comprising:

information accumulating unit to accumulate the value data, a transfer key used to update the value data, and an update key used to update the transfer key;

communication unit to receive a transfer key encrypted by use of the update key, said transfer key being transmitted from said another smart card; and

arithmetic processing unit to decrypt the encrypted transfer key by use of the update key to update the transfer key accumulated in the information accumulating unit by use of the decrypted transfer key.

18. A smart card that transmits/receives value data to/from another smart card, said smart card comprising:

information accumulating unit to accumulate the value data, a transfer key used to update the value data, and a secret key based on public-key cryptography, said secret key being used to update the transfer key;

communication unit to receive a transfer key encrypted using a public key corresponding to the secret

key, said transfer key being transmitted from said another smart card; and

arithmetic processing unit to decrypt the encrypted transfer key by use of the secret key to update the transfer key accumulated in the information accumulating unit by use of the decrypted transfer key.

19. A settlement terminal that transmits/receives first value data accumulated in a first smart card and second value data accumulated in a second smart card between the first smart card that accumulates a first transfer key used to update the first value data and an update key used to update the first transfer key, and the second smart card that accumulates a second transfer key used to update the second value data and an update key used to update the second transfer key, said settlement terminal comprising:

first smart-card read/write unit, if the first transfer key differs from the second transfer key, for receiving the first transfer key encrypted by use of the update key from the first smart card; and

second smart-card read/write unit to transmitt, to the second smart card, a transfer-key update request requesting that the second transfer key of the second smart card is updated to the first transfer key, said transfer-key update request including the first transfer key encrypted by use of the update key.

Abstract of the Disclosure

An object of the present invention is to provide a smart card and a settlement terminal by which, when common-key cryptography is used for value transfer between smart cards, the security of the whole system can be improved by enabling easy updating of a cryptographic key used for the value transfer.

A smart card transmits/receives value data to/from another smart card. The smart card includes information accumulating means for accumulating the value data, a transfer key used to update the value data, and an update key used to update the transfer key; a communication means for receiving a transfer key encrypted by use of the update key, the transfer key being transmitted from another smart card; and arithmetic processing means for decrypting the encrypted transfer key by use of the update key to update the transfer key accumulated in the information accumulating means by use of the decrypted transfer key.